

SECURITY POLICY – GARRY MERCER TRUCKING INC.

1. Effective date

June 1, 2005

2. Preamble

Garry Mercer Trucking Inc. depends on its personnel and assets to deliver services that ensure the health, safety, security and economic well-being of our customers, interliners and suppliers. It must manage these resources with due diligence and take appropriate measures to safeguard them and ourselves from injury.

The threats that can cause injury to Mercer personnel and assets, in Canada and abroad, include violence toward employees, unauthorized access, theft, fraud, vandalism, fire, natural disasters, technical failures and accidental damage.

The Mercer Security Policy prescribes the application of safeguards to reduce the risk of injury. It is designed to protect employees, preserve the confidentiality, integrity, availability and value of assets, and assure the continued delivery of services.

3. Policy objective

To support Garry Mercer Trucking Inc.'s business objectives by safeguarding employees and assets and assuring the continued delivery of services.

4. Policy statement

Employees under threat of violence must be safeguarded according to baseline security requirements and continuous security risk management.

Assets must be safeguarded according to baseline security requirements and continuous security risk management.

Continued delivery of services must be assured through baseline security requirements, including business continuity planning, and continuous security risk management.

5. Application

This policy applies to all departments and branches of Garry Mercer Trucking Inc.

6. Accountability

Department heads are accountable for safeguarding employees and assets under their area of responsibility and for implementing this policy.

7. Supporting documentation

This policy is supplemented by:

The Professional Driver Manual and the Profiles of Shippers, Interliners and Suppliers.

8. Requirements

Departments must comply with the baseline requirements of this policy and its associated operational standards and technical documentation. These requirements are based on integrated assessments of threats and risks to Mercer employees and assets. Departments must conduct their own threat and risk assessments to determine the necessity of safeguards above baseline levels.

The requirements of this policy complement other Mercer measures on the management of emergency situations (e.g., fire, bomb threats, hazardous materials, power failures, evacuations, civil emergencies).

Garry Mercer Trucking Inc. may direct departments to implement heightened security levels in emergency or increased threat situations.

8.1 Security program

Departments must appoint a Departmental Security Officer (DSO) to establish and direct a security program that ensures co-ordination of all policy functions and implementation of policy requirements. These functions include general administration (departmental procedures, training and awareness, identification of assets, security risk management, sharing of information and assets), access limitations, security screening, physical security, protection of employees, information technology security, security in emergency and increased threat situations, business continuity planning, security in contracting and security incident investigations.

Given the importance of this role, consideration should be given to appointing a Departmental Security Officer with sufficient security experience who is strategically positioned within the organization so as to provide department-wide strategic advice and guidance to senior management.

8.2 Sharing of information

In an effort to heighten the effectiveness of this policy we will actively share this information with our customers, interliners and suppliers. Mercer will encourage them to participate and will make them aware of our policies.

8.3 Security outside of Canada

Restrictions may be placed on personal activities at locations where the environment is particularly dangerous. All employees are automatically subject to local laws and regulations. Employees must be aware that serious breaches of local laws abroad can, under Canadian law, be prosecuted in Canada.

8.4 Contracting

This policy applies equally to the contracting process as it does to internal Mercer operations. The Department contracting must:

- a. Ensure security screening of organizations and individuals who have access to protected information and assets, as specified in the standards.
- b. Ensure safeguarding of Mercer assets, including IT systems.
- c. Specify the necessary security requirements in terms and conditions in any contractual documentation.

8.5 Security training, awareness and briefings

Departments must:

- a. Ensure that individuals who have specific security duties receive appropriate, up to date training.
- b. Have a security awareness program to inform and regularly remind individuals of security responsibilities, issues and concerns.
- c. Brief individuals on the access privileges and prohibitions prior to commencement of duties, or when required in the update cycle.

8.6 Identification of assets

Assets include, but are not limited to, equipment, facilities, freight, data bases and information and our ability to move freight across the Canada / USA border.

Availability, Integrity and Value

Departments must identify and categorize assets, especially critical services, based on the degree of injury (low, medium, high) that could reasonably be expected to result from compromise to their availability or integrity. They must consider the value of assets in determining injury. In order to indicate the level of safeguarding, departments should consider marking for availability and integrity purposes.

8.7 Security risk management

Departments must conduct ongoing assessments of threats and risks to determine the necessity of safeguards beyond baseline levels. They must continuously monitor for any change in the threat environment and make any adjustment necessary to maintain an acceptable level of risk and a balance between operational needs and security.

Threat and risk assessments involve:

- a. Establishing the scope of the assessment and identifying the employees and assets to be safeguarded (see sections 10.6 and 10.10).
- b. Determining the threats to employees and assets in Canada and abroad, and assessing the likelihood and impact of threat occurrence.
- c. Assessing the risk based on the adequacy of existing safeguards and vulnerabilities.
- d. Implementing any supplementary safeguards that will reduce the risk to an acceptable level.

8.8 Access limitations

Departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information. To the extent necessary, they must also limit access to other assets requiring additional safeguarding for availability, integrity or value purposes. This includes ensuring that no one individual can independently control all aspects of a process or a system.

8.9 Security screening

Garry Mercer Trucking Inc. must ensure that individuals with access to Mercer information and assets are reliable and trustworthy. Special care must be taken to ensure the continued reliability and loyalty of individuals.

Departments must ensure that, prior to the commencement of duties, individuals who require:

- a. Access to Mercer assets undergo a reliability check and are granted a reliability status.
- b. Access to information and assets have a valid reliability status, undergo a security assessment.
- c. Access to facilities should be limited to those areas required to performing the individual's duties.
- d. Drivers are subject to screening as laid out in the Professional Driver Manual.

Departments must also:

- a. Obtain individuals' written consent before any check may be initiated.
- b. Treat individuals in a fair and unbiased manner, and give them an opportunity to explain adverse information before a decision is reached.
- c. Advise individuals of their rights of review or redress in case of denial, suspension or revocation.
- d. Ensure managers remain vigilant, once a reliability status is granted, and act on any new information that could put into question an individual's reliability or loyalty.
- e. Update reliability status regularly.
- f. Compromise of reliability status can be grounds for dismissal.

8.10 Protection of employees

Departments are responsible under the *Canada Labour Code*, Part II for the health and safety of employees at work. This responsibility extends to situations where employees are under threat of violence because of their duties or because of situations to which they are exposed. Such situations include, but are not limited to threat letters or calls, the receipt of potentially dangerous substances, stalking and assault.

Departments must have in place mechanisms to:

- a. Identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases, protection and support may have to be extended to family members and others.
- b. Report incidents to management, human resources, security and police authorities, as may be the case.
- c. Provide information, training, and counseling to employees.
- d. Maintain thorough records and statements on reported incidents.

8.11 Cargo security

Any and all cargo tendered to Mercer Trucking will be inspected by a responsible Mercer employee to insure that it conforms to documentation. Deviation in content, dimensions, weight, description or quantity will be investigated and resolved prior to the movement of the cargo. Seals and / or locks will be used on all trailers to ensure that freight can not be tampered with.

Profiling of Shippers security and physical inspection of their facilities will be conducted on an ongoing basis for those shippers interfacing directly with Mercer. Freight Brokers, Forwarders, and 3PLs will be required to conduct and supply Shipper Profiles for those shippers who do not interface directly with Mercer.

8.12 Physical security

Physical security involves the proper layout and design of facilities and the use of measures to delay and prevent unauthorized access to Mercer assets. It includes measures to detect attempted or actual unauthorized access, and activate an appropriate response. Physical security also provides measures to safeguard employees from violence.

Access to Mercer information and assets will require the designation of a responsible employee to supervise any and all visitors, drivers, contractors, and suppliers.

Continuous review of physical security safeguards is essential to reflect changes in the threat environment and take advantage of new cost-effective technologies.

8.13 Information technology security

Information systems must be secured against rapidly evolving threats that have the potential to impact their confidentiality, integrity, availability, intended use and value. To defend against these threats, an IT security (ITS) strategy is required that accommodates changes in threat conditions, which may be sudden, and supports the continuous delivery of services. This dictates that departments apply baseline security controls, continuously monitor service delivery levels, track and analyse threats to departmental IT systems, and establish effective incident response and IT continuity mechanisms.

8.13.1 Prevention

To prevent the compromise of IT systems, departments must implement baseline security controls and any additional control identified through a threat and risk assessment. These controls, and the security roles and responsibilities of all personnel, must be clearly defined, documented and communicated to the general staff.

8.13.2 Detection

Since services may rapidly degrade due to computer incidents, ranging from a simple slowdown to a complete halt, departments must continuously monitor the operations of their systems to detect anomalies in service delivery levels.

8.13.3 Response

Departments must:

- a. In the context of investigation of security incidents (section 10.15), establish mechanisms to respond effectively to IT incidents and exchange incident-related information with designated lead departments in a timely fashion.
- b. Designate an IT security point of contact for communications with respect to Mercer-wide incident response.

8.13.4 Recovery

To ensure the ongoing availability of critical services, departments must develop IT continuity plans as part of their overall business continuity planning and recovery activities.

8.14 Security in emergency and increased threat situations

Departments must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. Garry Mercer Trucking Inc. may direct departments to implement heightened security levels.

Departments must co-ordinate these plans with other emergency prevention and response plans (e.g., fire, bomb threats, hazardous materials, power failures, evacuations, civil emergencies).

8.15 Business continuity planning

Critical services and associated assets must remain available in order to assure the health, safety, security and economic well-being of our customers, interliners and suppliers, and the effective functioning of Mercer Trucking. Departments must establish a business continuity planning (BCP) program to provide for the continued availability of service and assets, and of other services and assets when warranted by a threat and risk assessment.

The program shall include the following elements:

- a. Within the context of the departmental security program and organization (section 10.1), a governance structure establishing authorities and responsibilities for the program, and for the development and approval of business continuity plans.
- b. Within the context of the identification of assets (section 10.6), an impact analysis to identify and prioritize the department's critical services and assets.
- c. Plans, measures and arrangements to ensure the continued availability of critical services and assets, and of any other service or asset when warranted by a threat and risk assessment.
- d. Activities to monitor the department's level of overall readiness.
- e. Provision for the continuous review, testing and audit of business continuity plans.

8.16 Investigation of Security Incidents

Through effective reporting and investigation of security incidents, vulnerabilities can be determined and the risk of future occurrence reduced.

Departments must develop procedures for reporting and investigating security incidents and taking corrective action.

They must also report:

- a. Incidents suspected of constituting criminal offences to the appropriate law enforcement authority.
- b. Incidents that have an impact on Mercer operations or that could require revisions to operational standards or technical documentation.

8.17 Sanctions

Departments are required to apply sanctions in response to security incidents when in the opinion of the Department head there has been misconduct or negligence.

9. Monitoring

Departments are required to conduct active monitoring and internal audits of their security program. Further, Profiles of Shippers, Interliners and Suppliers are subject to auditing on an annual basis or as situational changes warrant. The results of internal audits must be reported to the Safety and Compliance Manager.

10. Review

This policy will be reviewed annually.

